



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/543,056	04/05/2000	Daniel R. Simon	MS1-406US	7223
22801	7590	02/13/2004	EXAMINER	
LEE & HAYES PLLC 421 W RIVERSIDE AVENUE SUITE 500 SPOKANE, WA 99201			MCARDLE, JOSEPH M	
			ART UNIT	PAPER NUMBER
			2132	4
DATE MAILED: 02/13/2004				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/543,056

Applicant(s)

SIMON, DANIEL R.

Examiner

Joseph McArdle

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 4/5/2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-6, 9-14, 17-24 and 26-30 is/are rejected.
- 7) ☒ Claim(s) 7, 8, 15, 16 and 25 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 05 April 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 2.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 18, 19, 21, 22, 26 are rejected under 35 U.S.C. 102(e) as being anticipated by Goldschlag (6108644). In regards to claim 18, Goldschlag discloses a design in column 5, lines 45-50 and in figure 1, in which a first party (client device) sends a blinded certificate to a registrar (certifying authority). Goldschlag then discloses in column 5, lines 56-60, that the registrar (certifying authority) will determine if the data received from the first party (client device) is valid and if it is then the registrar will sign the blinded certificate. These disclosures meet the limitations set forth under claim 18, which call for having an apparatus to digitally sign and encode electronic information that is received from a client including attributes of the client device. Goldschlag further discloses in column 6, lines 10-13, that a secure channel is used to communicate information between the user (client) and the registrar (certifying authority). This meets the remaining limitation set forth under claim 18, which calls for having a connection module to establish a secure connection with the client.
2. In regards to claim 19, Goldschlag further discloses in column 5, lines 51-53 that authorization data, such as a password and access codes are included in the validated (signed) certificate. This meets the limitations set forth under claim 19 because the

authorization data described above is representative of security attributes of the client device.

3. In regards to claim 21, Goldschlag discloses in column 4, lines 48-56, that a customer submits a validated (signed) certificate to a third party vendor in order to receive goods or services (such as electronic content). This meets the first limitation set forth under claim 21, which calls for receiving a request for electronic content from a client. Goldschlag further discloses in the same location as mentioned above that the vendor will determine if the client provided certificate is valid and determine whether or not to provide the requested goods or services (such as electronic content). This meets the remaining limitations set forth under claim 21, which call for checking the digital signature to determine its validity and then providing electronic content based on the results of the validity check.

4. In regards to claim 22, Goldschlag further discloses in column 4, lines 48-56, that if the validated (signed) unblinded certificate submitted to the vendor (content server) by the first party (client) is valid, then a response action is taken such as providing a service. This disclosure meets the exact limitations set forth under claim 22.

5. In regards to claim 26, Goldschlag further discloses in column 11, lines 1-13 that transaction instructions are stored on computer-readable mediums. This meets the exact limitations set forth under claim 26.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-6, 10-14, 17, 20, 23, 24, 27-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goldschlag (6108644) in view of Geer (6212634). In regards to claim 1, Goldschlag discloses a design in column 5, lines 45-50 and in figure 1, in which a first party (client device) sends a blinded certificate to a registrar (certifying authority). Goldschlag then discloses in column 5, lines 56-60, that the registrar (certifying authority) will determine if the data received from the first party (client device) is valid and if it is then the registrar will sign the blinded certificate. These disclosures meet the limitations set forth under claim 1, which call for having a client device coupled to a certifying authority (column 5, lines 45-50 and figure 1) so that the client device can transmit a blinded certificate to the certifying authority and have it validated and signed (see column 5, lines 56-60). However, Goldschlag makes no mention of allowing the client to generate a blinded certificate that includes a public key. Geer teaches in column 1, lines 8-17, that it is known to have certifying authorities generate certificates based upon the public keys of the parties attempting to become certified or verified. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Geer's teachings on the use of public keys used in a certification/validation process into Goldschlag's design in order to achieve a design that is capable of allowing a client device to include its public key in a blinded certificate that it generates and sends to a certifying authority.

3. In regards to claim 2, Goldschlag further discloses in column 2, lines 52-58, that the first party (client) unblinds the validated (signed) blinded certificate received from the second party (certifying authority). This disclosure meets the exact limitations set forth under claim 2, which call for the client device (first part in Goldschlag reference) to unblind the signed blinded certificate.

4. In regards to claim 3, Goldschlag further discloses in column 4, lines 47-56, that a vendor is used to provide the first party (client) with goods or services. This meets the limitations set forth under claim 3 because the vendor is acting as a content server as called for by claim 3 and is capable of delivering electronic content.

5. In regards to claim 4, Goldschlag discloses in column 4, lines 47-56, that a first party (client) sends the unblinded validated (signed) certificate (obtained by the method disclosed in the rejection of claim 2) to a vendor (content server), who determines whether the certificate is valid and accordingly formulates a response action. This meets the limitations set forth under claim 4, which calls for having a client device transmit the unblinded signed certificate to the content server, which then determines an appropriate response.

6. In regards to claim 5, Goldschlag further discloses in column 4, lines 48-56, that if the validated (signed) unblinded certificate submitted to the vendor (content server) by the first party (client) is valid, then a response action is taken such as providing a service. This disclosure meets the exact limitations set forth under claim 5.

7. In regards to claim 9, Goldschlag further discloses in column 5, lines 45-50 and in figure 1, that a client sends a blinded certificate to a registrar (certifying authority).

Goldschlag then discloses in column 5, lines 56-60, that the registrar (certifying authority) will determine if the data received from the first party (client) is valid, and if it is valid then the registrar will sign the blinded certificate to create a newly signed blinded certificate. These disclosures meet the first limitations set forth under claim 9, which call for receiving a current certificate from a client along with a request to sign a new one (see column 5, lines 45-50 and figure 1) and determining whether the current certificate received from the client is valid based upon client attributes. However, Goldschlag makes no mention of selecting a public/private key pair that is based at least in part on the attributes of the client and also signing the new certificate with the selected private key. Geer teaches in column 1, lines 8-10, that it is known to have certifying authorities that generate public key certificates that are enciphered with the private key of the certifying authority. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Geer's teachings on the use of public/private key pairs into Goldschlag's design in order to achieve a design that is capable of having a public/private key pair that is based at least in part on the attributes of the client and also signing the new certificate with the private key.

8. In regards to claim 10, Goldschlag further discloses in column 5, lines 51-53, that authorization data such as passwords and access codes are included in the certificate. This meets the limitations set forth under claim 10 because the authorization data described above is representative of security attributes of the client device.

9. In regards to claim 11, Goldschlag further discloses in column 5, lines 59-64, that the registrar (certifying authority) signs the certificate to create a new validated blinded

certificate. This meets the exact limitations set forth under claim 11, which calls for the certificate to be blinded.

10. In regards to claim 12, Goldschlag further discloses in column 5, lines 45-53, the use of authorization data that is included in the certificate that is to be signed. This authorized data meets the limitations set forth under claim 12 that call for determining additional information that can be encoded in the digital signature. However, Goldschlag makes no mention of selecting a public/private key pair based on the additional information. Geer teaches in column 1, lines 8-10, that it is known to have certifying authorities that generate public key certificates that are enciphered with the private key of the certifying authority. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Geer's teachings on the use of public/private key pairs into Goldschlag's design in order to achieve a design that is capable of selecting the public/private key pair based on the attributes of the additional information.

11. In regards to claim 13, Goldschlag further discloses in column 5, lines 51-53, that authorization data, such as password and access codes are included in the certificate. These passwords and access codes are representative of security attributes associated with the client and they would conform to specific bit patterns. This disclosure meets the first limitations set forth under claim 13 that call for determining a bit pattern that corresponds to the security attributes of the client. However, Goldschlag makes no mention of identifying a public/private key pair that corresponds to the bit pattern. Geer teaches in column 1, lines 8-10, that it is known to have certifying authorities that

generate public key certificates that are enciphered with the private key of the certifying authority. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Geer's teachings on the use of public/private key pairs into Goldschlag's design in order to achieve a design that is capable of identifying a public/private key pair that corresponds to the bit pattern.

12. In regards to claims 17, 28, and 30, Goldschlag further discloses in column 11, lines 1-13 that transaction instructions are stored on computer-readable mediums. This meets the exact limitations set forth under claims 17, 28, and 30.

13. In regards to claim 20, Goldschlag discloses in column 4, lines 47-56, that a first party (client) sends the unblinded validated (signed) certificate (obtained by the method disclosed in the rejection of claim 2) to a vendor (certificate archive), who determines whether the current certificate is valid and accordingly formulates a response action. This meets the limitations set forth under claim 20 that call for having a client device transmit the unblinded signed certificate to certificate archive, which then determines an appropriate response based on whether or not the current certificate is valid. However, Goldschlag makes no mention of using a received public key in order to determine whether the current certificate is valid. Geer teaches in column 1, lines 8-17, that it is known to have certifying authorities generate certificates based upon the public keys of the parties attempting to become certified or verified. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Geer's teachings on the use of public keys used in a certification/validation process into

Goldschlag's design in order to achieve a design that is capable of allowing a certificate archive to receive a public key and use it to validate a certificate.

14. In regards to claim 23, Goldschlag further discloses in column 5, lines 51-53 that authorization data, such as a password and access codes are included in the validated (signed) certificate. This meets the limitations set forth under claim 23 that call for having a set of security attributes because the authorization data described above is representative of security attributes of the client device. However, Goldschlag makes no mention of determining a public key based on these security attributes and then using the public key to verify the digital signature. Geer teaches in column 1, lines 8-10, that it is known to have certifying authorities that generate public key certificates that are enciphered with the private key of the certifying authority. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Geer's teachings on the use of public/private key pairs into Goldschlag's design in order to achieve a design that is capable of determining a public key that corresponds to the security attributes and using the public key to verify the digital signature.

15. In regards to claim 24, Goldschlag further discloses in column 5, lines 51-53, that authorization data, such as password and access codes are included in the certificate. These passwords and access codes are representative of security attributes associated with the client and they would conform to specific bit patterns. This disclosure meets the limitations set forth under claim 24 that call for determining a bit pattern that corresponds to the security attributes of the client. However, Goldschlag makes no mention of identifying a public/private key pair that corresponds to the bit pattern. Geer

teaches in column 1, lines 8-10, that it is known to have certifying authorities that generate public key certificates that are enciphered with the private key of the certifying authority. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Geer's teachings on the use of public/private key pairs into Goldschlag's design in order to achieve a design that is capable of identifying a public/private key pair that corresponds to the bit pattern and using the public key to verify the digital signature.

16. In regards to claim 27, Goldschlag discloses in column 4, lines 47-56, that a first party (client) sends the unblinded validated (signed) certificate (obtained by the method disclosed in the rejection of claim 2) to a vendor (certificate archive), who determines whether the current certificate is valid and accordingly formulates a response action. This meets the limitations set forth under claim 27 that call for having a client device transmit the unblinded signed certificate to certificate archive, which then determines an appropriate response based on whether or not the current certificate is valid. However, Goldschlag makes no mention of using a received public key in order to determine whether the current certificate is valid. Geer teaches in column 1, lines 8-17, that it is known to have certifying authorities generate certificates based upon the public keys of the parties attempting to become certified or verified. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Geer's teachings on the use of public keys used in a certification/validation process into Goldschlag's design in order to achieve a design that is capable of allowing a certificate archive to receive a public key and use it to validate a certificate.

17. In regards to claim 29, Goldschlag discloses in column 4, lines 47-56, that a first party (client) sends the unblinded validated (signed) certificate (obtained by the method disclosed in the rejection of claim 2) to a vendor (certificate archive), who determines whether the current certificate is valid and accordingly formulates a response action. This meets the limitations set forth under claim 29 that call for having a client device transmit the unblinded signed certificate to certificate archive, which then determines an appropriate response based on whether or not the current certificate is valid. However, Goldschlag makes no mention of generating public/private key pairs that use public keys to generate certificates over and over depending on whether the previous certificate was valid or not. Geer teaches in column 1, lines 8-17, that it is known to have certifying authorities generate certificates based upon the public keys of the parties attempting to become certified or verified. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Geer's teachings on the use of public keys used in a certification/validation process into Goldschlag's design in order to achieve a design that is capable generating new certificates based public keys if it is determined that previous certificates were not valid.

18. Claims 6 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goldschlag and Geer as applied to claims 1 and 9 above, and further in view of Chaum (4759063). Goldschlag and Geer's design disclosed above meets all of the aforementioned limitations of claims 1 and 9 above. However, Goldschlag and Geer's design makes no mention of signing the blinded certificate according to the formula:

Art Unit: 2132

(blinded certificate)^d mod (*n*), wherein *d* represents a private key of the certifying authority and *n* is the product of two prime numbers. Chaum teaches in column 1, lines 52-64, that the function $f(x) = x^e \text{ mod } (n)$ can be used to apply a secure digital signature because it is almost impossible to compute *d* (representative of the key) from *n* (product of two primes) without knowing the prime factors that were involved in computing *n*. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Chaum's teachings on applying secure digital signatures into Goldschlag and Geer's design in order to achieve a design that is capable of signing the blinded certificate according to the formula (blinded certificate)^d mod (*n*).

Allowable Subject Matter

Claims 7, 8, 15, 16, and 25 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent Chaum (4949380)

U.S. Patent Sudia (5659616)

U.S. Patent Brands (6052467)

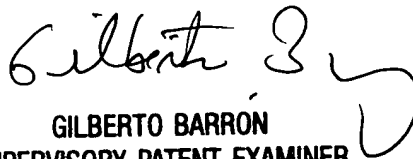
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph McArdle whose telephone number is (703) 305-7515. The examiner can normally be reached on Weekdays from 8:00 am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


jmm

Joseph McArdle
Examiner
Art Unit 2132


GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100